

ORIGINAL

FILED
U.S. DISTRICT COURT
NORTHERN DIST. OF TX
FT. WORTH DIVISION

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS,
FORT WORTH DIVISION**

2015 MAY -1 PM 2:58

CLERK OF COURT

TPG GLOBAL, LLC, a limited
liability company,

Plaintiff,

v.

ADAM LEVINE, an individual,

Defendant.

§
§
§
§
§
§
§
§
§

NO. 4:15-CV-00059-A

**DEFENDANT'S BRIEF IN SUPPORT OF MOTION
TO DISMISS SECOND AMENDED COMPLAINT**

TABLE OF CONTENTS

Index of Authorities	ii
BACKGROUND	1
ARGUMENT AND AUTHORITIES.....	1
I. Plaintiff's allegations do not state an "unauthorized access" claim under the CFAA.....	2
A. Plaintiff has alleged neither that Levine accessed a computer without authorization or that he exceeded his authorized access.	3
B. The Fifth Circuit has not embraced a view of the CFAA that is wide enough to allow Plaintiff's "exceeds authorized access" claims.....	4
II. Plaintiff's allegations do not state a "transmission" claim under the CFAA.....	8
III. Plaintiff's allegations do not state a claim under the CFAA for lost data on Levine's laptop or Blackberry.	9
IV. Plaintiff has not adequately alleged a "loss" aggregating \$5,000 or more as required to state a claim under the CFAA.....	10
CONCLUSION AND PRAYER	13
CERTIFICATE OF SERVICE	14

INDEX OF AUTHORITIES

Cases

<i>Adamo Wrecking Co. v. United States</i> , 434 U.S. 275 (1978)	2
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)	1, 2
<i>B.U.S.A. Corp. v. Ecogloves, Inc.</i> , No. 05 Civ. 9988, 2009 U.S. Dist. LEXIS 89035 (S.D.N.Y. Sept. 28, 2009)	10
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007)	1, 11
<i>Bose v. Interclick, Inc.</i> , No. 10 Civ. 9183 (DAB) 2011 U.S. Dist. LEXIS 93663 (S.D.N.Y. Aug. 17, 2011)	11
<i>Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int’l. Inc.</i> , 616 F.Supp.2d 805 (N.D. Ill. 2009)	12
<i>EF Cultural Travel BV v. Explorica, Inc.</i> , 274 F.3d 577 (1st Cir. 2001)	4, 6, 7
<i>Garland-Sash v. Lewis</i> , No. 05 Civ. 6827, 2011 U.S. Dist. LEXIS 143626 (S.D.N.Y. Dec. 6, 2011)	10, 11
<i>In re Google Inc. Cookie Placement Consumer Privacy Litigation</i> , 988 F.Supp.2d. 434 (D. Del. 2013)	8
<i>International Airport Centers, LLC v. Citrin</i> , 440 F.3d 418 (7th Cir. 2006)	4
<i>International Chauffeured Serv., Inc. v. Fast Operating Corp.</i> , No. 11 Civ. 2662 (NRB) 2012 WL 1279825 (S.D.N.Y. April 16, 2012)	10, 11
<i>Leocal v. Ashcroft</i> , 543 U.S. 1 (2004)	3
<i>LVRC Holdings LLC v. Brekka</i> , 581 F.3d 1127 (9th Cir. 2009)	7
<i>Nexans Wires S.A. v. Sark-USA, Inc.</i> , 319 F. Supp. 2d 468 (S.D.N.Y. 2004), <i>aff’d</i> 166 F. App’x 559 (2d Cir. 2006)	11
<i>OCE North Am., Inc. v. MCS Servs., Inc.</i> , 748 F.Supp.2d 481 (D. Md. 2010)	5
<i>Rewis v. United States</i> , 401 U.S. 808 (1971)	2
<i>United States v. Aleynikov</i> , 676 F.3d 71 (2nd Cir. 2012)	5

<i>United States v. John</i> , 597 F.3d 263 (5th Cir. 2010)	5, 6
<i>United States v. Nosal</i> , 676 F.3d 854 (9th Cir. 2012).....	5
<i>United States v. Reedy</i> , 304 F.3d 358 (5th Cir. 2002), reh'g denied (2002)	2
<i>University Sports Pubs. Co. v. Playmakers Media Co.</i> , 725 F.Supp.2d 378 (S.D.N.Y. 2010)	5
<i>WEC Carolina Energy Solutions LLC v. Miller</i> , 687 F.3d 199 (4th Cir. 2012), cert. denied 133 S. Ct. 831 (2013)	2, 5

Statutes

18 U.S.C. § 1030(a)(2)(C)	3, 4
18 U.S.C. § 1030(a)(5)(A)	8, 9
18 U.S.C. § 1030(a)(5)(C)	4, 9
18 U.S.C. § 1030(e)(6).....	4
18 U.S.C. § 1030(e)(8).....	8
18 U.S.C. § 1030(g)	2, 10
Fed. R. Civ. P. 8(a)(2).....	1

Defendant Adam Levine moves the Court to dismiss Plaintiff's Second Amended Complaint because it fails to state a claim under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (CFAA) and because, absent a viable claim under that statute, there is no basis for subject matter jurisdiction over the remaining claims.

BACKGROUND

TPG Global filed its Complaint and First Amended Complaint in January 2015, alleging that Levine breached state-law duties regarding confidentiality of information to which he had access while Plaintiff's employee. Levine moved to dismiss for lack of personal jurisdiction and lack of subject matter jurisdiction based on diversity. In response, Plaintiff filed a Second Amended Complaint that adds ten new parties and a new federal cause of action under the CFAA. This new claim, which is Plaintiff's sole basis for invoking this Court's subject matter jurisdiction, does not afford Plaintiff the possibility of any additional relief. If viable, however, it elevates to a federal crime every garden-variety claim that an employee violated a computer-use policy. This is too high a price for Plaintiff's ticket to federal court and is not what Congress intended when enacting the CFAA to punish hackers and other computer criminals.

ARGUMENT AND AUTHORITIES

Federal Rule of Civil Procedure 8(a)(2) requires a complaint to contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). The "showing" contemplated by this rule requires Plaintiff to do more than simply allege legal conclusions or recite the elements of its cause of action. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). Although the Court must accept all of the factual allegations in the Second Amended Complaint as true, it need not credit bare legal conclusions that are unsupported by any factual underpinnings. *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009). In addition, the facts pleaded must allow the Court to infer that Plaintiff's right to relief is plausible.

Id. at 678. “Determining whether a complaint states a plausible claim for relief . . . [is] a context-specific task that requires the reviewing court to draw on its judicial experience and common sense.” *Id.* at 679.

Plaintiff’s attempt to cast its claims as four or five violations of the CFAA falls short of these requirements. As shown in section I below, paragraphs 87, 88, and 89 of the Second Amended Complaint are inadequate to state claims because Plaintiff does not allege that Levine’s access to TPG’s computer system exceeded his authorization as that phrase is defined in the CFAA. Section II shows that paragraph 90 fails to state a claim because Plaintiff pleads no facts to show that Levine committed a “transmission” violation or intentionally caused “damage” as that term is defined in the CFAA. Section III demonstrates that Plaintiff has not stated a claim relating to Levine’s laptop and Blackberry. Finally, section IV shows that all of Plaintiff’s CFAA claims fail for the independent additional reason that Plaintiff does not plausibly allege that it suffered the nature and threshold amount of “loss” that is required to pursue a civil action under the CFAA.

I. Plaintiff’s allegations do not state an “unauthorized access” claim under the CFAA.

The CFAA is “primarily a criminal statute designed to combat hacking.” *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 201 (4th Cir. 2012), *cert. denied* 133 S. Ct. 831 (2013). While any violation of the Act constitutes a criminal offense, Congress provided a civil cause of action for a limited subset of those offenses. 18 U.S.C. § 1030(g).

Criminal statutes are narrowly construed. *See Adamo Wrecking Co. v. United States*, 434 U.S. 275, 285 (1978) (“where there is ambiguity in a criminal statute, doubts are resolved in favor of the defendant”); *Rewis v. United States*, 401 U.S. 808, 812 (1971) (“ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity”); *United States v. Reedy*, 304 F.3d 358, 367 (5th Cir. 2002) (*reh’g denied* 2002) (“ambiguity

should be resolved in favor of lenity”). Due to its hybrid nature, the CFAA is subject to strict and narrow construction in this civil action. *See Leocal v. Ashcroft*, 543 U.S. 1, 11 n. 8 (2004) (“we must interpret [a] statute consistently, whether we encounter its application in a criminal or noncriminal context”).

A. Plaintiff has alleged neither that Levine accessed a computer without authorization or that he exceeded his authorized access.

Three of Plaintiff’s CFAA claims, each stated in a single sentence, are “unauthorized access” claims. *See* 2nd Am. Compl. at ¶¶ 87-89. To state such a claim, Plaintiff must show either that Levine accessed a protected computer without authorization, or that his access to a protected computer exceeded his authorization. 18 U.S.C. §§ 1030(a)(2)(C); 1030(a)(4); 1030(a)(5)(C).

Although the Second Amended Complaint repeatedly asserts the bare legal conclusion that Levine “accessed TPG’s protected computer systems without authorization, and/or exceeding his authorized access,” 2nd Am. Compl. at ¶¶ 87-89, it alleges absolutely no facts to show that Levine’s access to any TPG computer was unauthorized. For example, Plaintiff does not allege that Levine stole a password, impersonated another user, or otherwise gained access to a computer that he was not entitled to use. To the contrary, Plaintiff affirmatively alleges that Levine “occupied a position of trust and confidence that afforded him access to sensitive nonpublic, confidential, and proprietary information about TPG and its business operations, including its strategic planning.” *Id.* at ¶ 22.

The question is thus whether Plaintiff adequately pleads that Levine exceeded his authorized access. This is a defined phrase in the CFAA. Congress provided that “the term ‘exceeds authorized access’ means to access a computer with authorization and to use such access to obtain or alter information that the accesser is not entitled so to obtain or alter.” 18

U.S.C. § 1030(e)(6). In support of its unauthorized access claims, Plaintiff does not allege that Levine altered information on any TPG computer. Nor does Plaintiff plead that Levine obtained any information that was beyond the scope of his authorized access. In fact, Plaintiff pleads precisely the opposite, stating that Levine “had access to the Firm’s *most sensitive* confidential and proprietary information.” 2nd Am. Compl. at ¶ 2 (emphasis added). Because the Second Amended Complaint alleges neither unauthorized access nor that Levine exceeded his authorized access, it does not state a claim under sections 1030(a)(2)(C), 1030(a)(4), and 1030(a)(5)(C) of the CFAA.

B. The Fifth Circuit has not embraced a view of the CFAA that is wide enough to allow Plaintiff’s “exceeds authorized access” claims.

Plaintiff will argue that Levine exceeded his authorized access by obtaining information for an unauthorized purpose (to breach his duty of confidentiality).¹ This argument conflicts with the CFAA definition that unauthorized access means obtaining information “that the accesser is not entitled so to obtain.” 18 U.S.C. § 1030(e)(6). But the argument does find support in some older opinions. *See, e.g., International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006) (holding that an employer’s authorization to use its computers is impliedly revoked when an employee uses the computer for a disloyal purpose); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001) (upholding a preliminary injunction based on allegations that a former employee breached his obligation to maintain confidentiality of his former employer’s information).

¹ For all of its vitriol, the Second Amended Complaint identifies only one piece of information that has allegedly been disclosed outside of TPG—an email of unidentified content that was allegedly sent to a New York Times reporter while Levine was still a TPG employee. 2nd Am. Compl. at ¶ 41. Plaintiff does not allege that the email was published in the paper or that TPG suffered any damages in connection with its alleged disclosure, but Plaintiff does affirmatively allege that Levine was among those who were authorized to access to the message. *Id.* at ¶ 42.

The majority of courts to consider the question, especially in the last several years, have opined that the CFAA is not intended to cover the common scenario in which an employee accesses information that he is authorized to access, but with a disloyal heart. These courts observe that the Act criminalizes unauthorized *access* and does not mention anything about improper *use*. They conclude that the CFAA is not broad enough to criminalize mere breach of confidentiality, for which the law recognizes myriad other remedies. *See, e.g., WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 207 (4th Cir. 2012), *cert. denied* 133 S. Ct. 831 (2013) (“we are unwilling to contravene Congress’s intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy”); *United States v. Nosal*, 676 F.3d 854, 857 (9th Cir. 2012) (“If Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions — which may well include everyone who uses a computer — we would expect it to use language better suited to that purpose.”); *United States v. Aleynikov*, 676 F.3d 71, 75 (2nd Cir. 2012) (“Count Three was dismissed on the ground that . . . authorized use of a computer in a manner that misappropriates information is not an offense under the Computer Fraud and Abuse Act.”). Innumerable district courts across the country have reached the same conclusion.²

The Fifth Circuit has staked out a unique middle ground. *See United States v. John*, 597 F.3d 263 (5th Cir. 2010). John was a Citibank employee who was convicted under the

² *See, e.g., University Sports Pubs. Co. v. Playmakers Media Co.*, 725 F.Supp.2d 378, 383 (S.D.N.Y. 2010) (stating that “Plaintiff’s theory runs afoul of a persuasive line of recent precedent,” and citing several cases); *OCE North Am., Inc. v. MCS Servs., Inc.*, 748 F.Supp.2d 481, 487 (D. Md. 2010) (discussing cases and concluding “it was part of [defendant’s] job to use Plaintiff’s computers and the software on the computers. As in *Orbit* and *Werner-Matsuda*, the fact that he copied the software on to his own laptop may have been a violation of his employment agreement, but that does not constitute a violation of the CFAA.”).

CFAA for copying customer account information and providing it to a co-conspirator to incur fraudulent charges on the customer accounts. She urged the Fifth Circuit to reverse her conviction on the ground that her position allowed her to access the customer account information, and the statute does not impose penalties simply because she used her access for the purpose of committing a brazen felony. The Court rejected this argument and affirmed John's conviction.

But the Court was careful to limit its holding in a way that does not criminalize the conduct alleged by Plaintiff here:

The question before us is whether “authorized access” or “authorization” may encompass limits placed on the use of information obtained by permitted access to a computer system and data available on that system. We conclude that it may, *at least when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime.*

Id. at 271 (emphasis added). Anticipating the application of its holding to the employment context, the Court was careful not to convert mere breach of employment contract into a crime: “an employer may ‘authorize’ employees to utilize computers for any lawful purpose but not for unlawful purposes and only in furtherance of the employer’s business. An employee would ‘exceed[] authorized access’ if he or she used that access to obtain or steal information *as part of a criminal scheme.*” *Id.* (emphasis added).

The Fifth Circuit expressed reservations about the First Circuit’s unqualified adoption of the “unauthorized use” interpretation. *Id.* at 272 (stating that “we do not necessarily agree that violating a confidentiality agreement under circumstances such as those in *EF Cultural Travel BV* would give rise to criminal culpability”). In addition, while recognizing that “the Ninth Circuit may have a different view of how ‘exceeds authorized access’ should be

construed”, *id.*, the Fifth Circuit agreed with that Court’s concern about converting common allegations of employee disloyalty into federal crimes:

The Ninth Circuit explained that “[i]f the employer has not rescinded the defendant’s right to use the computer, the defendant would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA. It would be improper to interpret a criminal statute in such an unexpected manner.”

There are no such concerns in the present case. An authorized computer user “has reason to know” that he or she is not authorized to access data or information in furtherance of a criminally fraudulent scheme. Moreover, the Ninth Circuit’s reasoning at least implies that when an employee knows that the purpose for which she is accessing information in a computer is *both* in violation of an employer’s policies *and is part of an illegal scheme*, it would be “proper” to conclude that such conduct “exceeds authorized access” within the meaning of § 1030(a)(2).

Id. at 272-73 (discussing and quoting *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009)) (emphasis added). Thus, the Fifth Circuit allows a claim based on unauthorized use or purpose only upon a showing that the defendant knowingly accessed information as part of a criminal scheme. Plaintiff does not allege that Levine used his access to TPG’s computers as part of a criminal scheme, much less that Levine did so knowingly.

Levine maintains that the Second, Fourth and Ninth Circuits have correctly interpreted the definition of “exceeds authorized access” to mean accessing information that the user is not authorized to access, without regard for the purpose of the access. But even under the Fifth Circuit’s somewhat broader view, Plaintiff has not stated a claim for access that exceeded authorization. At best, Plaintiff implies that Levine’s access to unidentified information was against TPG’s interests; but it wholly fails to allege that Levine’s access was knowingly in furtherance of a criminal scheme. On this basis, the Court should dismiss all of Plaintiff’s CFAA claims based on unauthorized access (paragraphs 87-89).

II. Plaintiff's allegations do not state a "transmission" claim under the CFAA.

Plaintiff's fourth CFAA claim is based section 1030(a)(5)(A), which makes it a crime to "knowingly cause[] the transmission of a program, information, program, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization to a protected computer." Plaintiff recites this statutory language in paragraph 90 of the Second Amended Complaint.

Plaintiff's single-sentence claim under this provision is based not on the transmission of a virus or destructive command, but on Levine "electronically submitting unauthorized expense reports." 2nd Am. Compl. at ¶ 90. This allegation was not in Plaintiff's original or first amended complaint, and it is not stated anywhere in the "FACTUAL BACKGROUND" section of the Second Amended Complaint. Plaintiff pleads no facts whatsoever to show that Levine ever submitted an unauthorized expense report.

Equally, if not more, deficient is Plaintiff's allegation that the "transmission" of some identified expense report intentionally caused "damage to TPG's protected computer systems." For the CFAA, Congress defined "damage" to mean "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Plaintiff alleges no facts whatsoever to show that the integrity or availability of any aspect of its computer system was intentionally impaired by the submission of the unidentified expense reports. *See generally In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 988 F.Supp.2d. 434, 448 (D. Del. 2013) (granting motion to dismiss because "Plaintiffs have not alleged the kind of damage or loss required to maintain a CFAA claim. More specifically, plaintiffs have not identified any impairment of the performance or functioning of their computers."). Plaintiff thus comes nowhere close to plausibly pleading a violation of section 1030(a)(5)(A).

III. Plaintiff's allegations do not state a claim under the CFAA for lost data on Levine's laptop or Blackberry.

Another brand new—and false—allegation in the Second Amended complaint is that Levine deleted all data from his laptop and Blackberry before returning them to TPG. In paragraph 92, Plaintiff alleges that “Levine knowingly caused damage to TPG’s computers and computer systems by, among other things, intentionally destroying all data and information contained on his TPG-owned laptop computer and Blackberry device.” Unlike the allegations in paragraphs 87 through 90, this allegation does not recite the elements of a CFAA claim. If Plaintiff is attempting to assert a violation of the CFAA based on this alleged deletion of data, the attempt fails.

There is no stand-alone federal crime for deletion of data. Instead, under circumstances not alleged here, deletion of data could possibly satisfy the “damage” element of a claim under section 1030(a)(5)(A) or 1030(a)(5)(C). But Plaintiff fails to allege the other elements of offenses under these two provisions in connection with its laptop and Blackberry accusations. Specifically, Plaintiff fails to allege knowing transmission as required to state a claim under section 1030(a)(5)(A) and fails to allege that Levine lacked authorization to access his laptop and Blackberry as required to state a claim under 1030(a)(5)(C).

Further, Plaintiff fails to plead any facts to show CFAA “damage” as a result of the alleged data deletion on the two remote devices. It alleges no impairment in the performance or functioning of its computer system. It does not assert the inherently implausible allegation that Levine’s remote devices contained the only copy of any TPG information or that the performance of TPG’s system somehow relies upon data that existed on Levine’s devices. In short, Plaintiff’s false allegation that Levine deleted data from the two devices before returning them to TPG fails to state an independent offense and civil claim under the CFAA.

IV. Plaintiff has not adequately alleged a “loss” aggregating \$5,000 or more as required to state a claim under the CFAA.

A final defect cuts across all of Plaintiff’s CFAA claims. The statute provides that “[a] civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i).” 18 U.S.C. § 1030(g). Plaintiff makes no attempt to plead that any asserted violation involves factor II (impairment of medical treatment), III (physical injury to a person), IV (threat to public health), or V (damage to a US Government computer). To state a claim, therefore, Plaintiff must adequately plead conduct involving factor I—“loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value.” *Id.* at § (c)(4)(A)(i)(I).

Congress defined “loss” under the CFAA to mean “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” *Id.* at § (e)(11). Cases analyzing these defined terms have held that merely accessing and copying data—even if unauthorized or for an improper purpose—does not result in “damage” to a computer system and cannot form the basis for a claim of “loss.”

A case that provides a good analysis of the statutory requirement and demonstrates the type of pleading specificity required to state a claim is *International Chauffeured Serv., Inc. v. Fast Operating Corp.*, No. 11 Civ. 2662 (NRB) 2012 WL 1279825 (S.D.N.Y. April 16, 2012). Dismissing a complaint with far more specific allegations that we have here, the court explained:

Courts construe “loss” narrowly, *B.U.S.A. Corp. v. Ecogloves, Inc.*, No. 05 Civ. 9988, 2009 U.S. Dist. LEXIS 89035, at *18 (S.D.N.Y. Sept. 28, 2009), and the term “includes only costs actually related to computers,” *Garland-Sash v. Lewis*, No. 05 Civ. 6827, 2011

U.S. Dist. LEXIS 143626, at *8-9 (S.D.N.Y. Dec. 6, 2011). Courts have interpreted the term to mean “any remedial costs of investigating the computer for damage, remedying the damage and any costs incurred because the computer cannot function while or until repairs are made.” *E.g., id.* at *9-10 (quoting *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 474 (S.D.N.Y. 2004), *aff’d* 166 F. App’x 559 (2d Cir. 2006)).

Id. at *3; *see also Bose v. Interclick, Inc.*, No. 10 Civ. 9183 (DAB) 2011 U.S. Dist. LEXIS 93663, at *12 (S.D.N.Y. Aug. 17, 2011) (explaining that “‘loss’ for the purposes of the CFAA, encompasses only ‘repair cost[s] or cost[s] associated with investigating the alleged damage’”).

Plaintiff attempts to satisfy the statute’s loss requirement in a single sentence referring to all four of its alleged offenses. It generically pleads: “As a result of Levine’s aforementioned unauthorized access of TPG’s computer systems, TPG has suffered damages in an amount to be proven at trial, but well in excess of \$5,000, which includes, but is not limited to, responding to the offense and assessing the damage caused to TPG’s computers and computer systems by Levine.” 2nd Am. Compl. at ¶ 91.³ Assuming Plaintiff means “loss” where it says “damages,” this allegation is deficient for three reasons.

First, Plaintiff has merely recited statutory elements in violation of *Twombly*, 550 U.S. at 555. It alleges no facts from which the Court could conclude that Plaintiff plausibly suffered a “loss” of at least \$5,000 in connection with any (much less each) of the four alleged offenses. Plaintiff fails to plead the nature of any specific costs incurred; to whom they were incurred; when they were incurred; or the amount(s) of any particular cost. Compare *International Chauffeured Service* at *1 (pleading that its “security investigation was performed

³ By pleading that its \$5,000 loss was the “result of the aforementioned unauthorized access of TPGS’s computer systems,” Plaintiff excludes the later-mentioned alleged destruction of data from the laptop and Blackberry. Nowhere does Plaintiff allege that conduct associated with these two devices resulted in a “loss” under the CFAA. For this additional reason, Plaintiff has not stated a claim based on the alleged destruction of data on the laptop and Blackberry.

by . . . the developer of the database, between October 19 and October 21 of 2009 at a cost of \$1413”). Plaintiff also fails to plead that any costs were reasonable, which the statute expressly requires, and without the underlying facts, there is no way for the Court or Levine to infer reasonableness.

Second, Plaintiff apparently cannot meet the \$5,000 threshold based on elements that the statute specifically identifies within the definition of “loss.” So it pleads that its \$5,000 loss “*includes, but is not limited to*, responding to the offense and assessing the damage caused to TPG’s computers.” 2nd Am. Compl. at ¶ 91 (emphasis added). Although unlisted elements of loss may be recoverable under the CFAA, and thus eligible to satisfy the \$5,000 threshold, the absence of factual allegations in Plaintiff’s Second Amended Complaint makes it impossible for the Court or Levine to infer that the other elements comprising Plaintiff’s alleged loss relate to TPG’s computers and qualify for recovery under the CFAA’s narrow definition of “loss.”

Third, Plaintiff pleads that it meets the \$5,000 threshold only by including the cost of “assessing the damage caused to TPG’s computers.” As discussed above, Congress defined “damage” in the CFAA to mean “impairment to the integrity or availability of data, a program, a system, or information.” *Id.* at § (e)(8). Thus, assessing damage is recoverable in cases alleging that the defendant impregnated the computer system with a virus, deleted data, or otherwise caused harm to the system components. Plaintiff has alleged only that Levine accessed and downloaded copies of files, which does not implicate impairment to the integrity or availability of data, a program, a system, or information. *See, e.g., Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int’l. Inc.*, 616 F.Supp.2d 805, 811 (N.D. Ill. 2009) (holding that “copying electronic files from a computer database—even when the ex-employee e-mails those files to a competitor—is not enough to satisfy the damage requirement of the CFAA; there must

be destruction or impairment to the integrity of the underlying data”). Therefore, the cost of assessing any such “damage” cannot be included in Plaintiff’s claimed “loss.” Because Plaintiff affirmatively alleges that it’s \$5,000 loss includes this cost, it has not pleaded a viable loss to support its causes of action under the CFAA.

Plaintiff’s failure to plead facts that plausibly show a “loss” of at least \$5,000 under the statute dooms all of its CFAA claims.

CONCLUSION AND PRAYER

For all of these reasons, Levine respectfully submits that Plaintiff has not successfully restated its state-law employment causes of action as claims for which it can obtain relief under the CFAA. Under Rules 8 and 12(b)(6), the federal claims should be dismissed. Because these claims are the only basis on which Plaintiff invokes this Court’s jurisdiction, the remaining state-law claims should be dismissed under Rule 12(b)(1). Defendant Levine therefore prays that the Court dismiss this case and award him such further relief to which he may be entitled.

Respectfully submitted,

Joseph R. Knight
Texas Bar No. 11601275
Law Office of Joseph R. Knight
111 Congress Ave., Suite 2800
Austin, Texas 78701
Telephone: (512) 457-0231
Fax: (512) 684-7681
Email: jknight@knighttxlaw.com

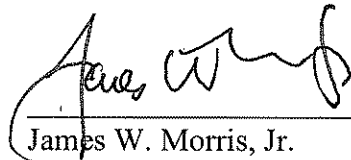
By: 
James W. Morris, Jr.
Texas Bar No. 14487600
MORRIS, SCHORSCH & STAPLETON PC
8080 N. Central Expressway, Suite 1300
Dallas, TX 75206
Telephone: (214) 888-3324
Fax: (214) 888-3327
Email: jmorris@msstxlaw.com

ATTORNEYS FOR DEFENDANT ADAM LEVINE

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing document was served by email and U.S. Mail on the following counsel of record on this 1st day of May, 2015

Constantine Z. Pamphilis
KASOWITZ, BENSON, TORRES & FRIEDMAN LLP
700 Louisiana Street, Suite 2200
Houston, Texas 77002
dpamphilis@kasowitz.com
Marc E. Kasowitz
KASOWITZ, BENSON, TORRES & FRIEDMAN LLP
1633 Broadway
New York, NY 10019
mkasowitz@kasowitz.com
MARSHALL M. Searcy, Jr.
KELLY HART & HALLMAN LLP
201 Main Street, Suite 2500
Fort Worth, Texas 76102
marshall.searcy@kellyhart.com


James W. Morris, Jr.